How to secure your machines - free

Inveniamviamaudacia

“Why this topic?”

- Security is a very complex area, but that is no reason to take simple steps
- Not getting 100% security should not stop you trying to achieve some at least
- What is wrong with making the bad guys work harder?
- Free does not mean bad, pricey does not mean good.
- Peace of mind should not be for those with cash
- Every secure machine is one less bot/spammer/etc

Inveniamviamautfaciam

"Web"

- First a decent browser – Firefox (http://www.mozilla.com/en-US/firefox/all-beta.html)
- Free, cross-platform, actively developed, built in patch management, etc
- Coolest thing is plugins. Ways to extend the functionality
- From a security point of view, 3 very useful additions to firefox (free)
  - Adblock Plus
  - Flashblock
  - Noscript
- Not only will you be more secure, but your browsing should be a little faster

“Email”

- Spambayes is a addon for outlook, outlook express, thunderbird, etc (http://spambayes.sourceforge.net/)
    - It allows for the training of a personal bayesian antispam ruleset

- GnuPG is for encryption, not just files but emails (http://gnupg.org/download/)
    - It allows for encryption and signing. Avalible for all OS’s.

- Thunderbird is a free cross-platform email client (http://www.mozilla.com/en-US/thunderbird/)
    - As a mozilla project it also features plugins and patch management

Inveniamviamautfaciam

“Anti-Virus”

- ClamAV is a well-known cross-platform AV engine (http://www.clamav.org/download/)
  - Well maintained, well used, the biggest drawback is no on-access scanning
  - But is free and used in many instances – snort, anti-spam, proxys, etc

- Comodo AV is a free non-ads windows only package (http://antivirus.comodo.com/)
  - While windows only, does do on-access, email, HIPS

- SpybotSD is a anti-malware windows only package (http://www.safer-networking.org/)
  - There are various free anti-malware tools but spybot is a front runner

“Privacy”

- Truecrypt is a cross-platform encrypted volume tool (http://www.truecrypt.org/)
  - Volumes can be mounted on various OS’s (filesystem dependant)
  - Can use keyfiles
  - Easy key management
  - Has a Traveller mode
  - Can do pre-boot authentication under windows

- OTR (Off-The-Record) a IM Client (Pidgin) encryption plugin (http://www.cypherpunks.ca/otr/)
  - Pidgin is a cross platform, multi protocol IM client
  - OTR gains cross platform use through using Pidgin

- Eraser is a windows tool to do secure deletions (http://www.heidi.ie/eraser/)
  - Can use various “grades” of deletion
  - Plugs in windows menu options
  - Can clear the “free” space of old data

Invenia mvia mautfacia m

“Advanced Topics”

- “Throw Away” virtual machines
  - Use a virtual machine to do work and web browsing (http://www.vmware.com/products/player/)
- Localhost firewalls
  - Both OSX and Linux have builtin options
  - Windows can use Comodo Firewall (http://www.personalfirewall.comodo.com/download_firewall.html)
- Network Traffic Privacy
  - A useful option here is TOR (http://www.torproject.org/)
  - Cross-platform again
  - Used for anonymity of traffic
- Virtual Private Network
  - OpenVPN is a SSL-based VPN (http://openvpn.net/)
  - Both server and client are cross platform

Invenia machina utfacia

Thank you for your attention

Inveniamviamautfaciam